

# Insecure Default File Permissions in Local Filesystem Memory Tool

**Moderate** localden published GHSA-q5f5-3gjm-7mfm 4 days ago

## Package

 anthropic (pip)

### Affected versions

>= 0.86.0, < 0.87.0

### Patched versions

0.87.0

## Description

The local filesystem memory tool in the Anthropic Python SDK created memory files with mode 0o666, leaving them world-readable on systems with a standard umask and world-writable in environments with a permissive umask such as many Docker base images. A local attacker on a shared host could read persisted agent state, and in containerized deployments could modify memory files to influence subsequent model behavior. Both the synchronous and asynchronous memory tool implementations were affected.

Users on the affected versions are advised to update to the latest version.

Thank you to [lucasfutures](#) on HackerOne for the report.

## Severity

**Moderate** 4.8 / 10

### CVSS v4 base metrics

#### Exploitability Metrics

Attack Vector	Local
Attack Complexity	Low
Attack Requirements	None
Privileges Required	Low

User interaction None

**Vulnerable System Impact Metrics**

Confidentiality Low

Integrity Low

Availability None

**Subsequent System Impact Metrics**

Confidentiality None

Integrity None

Availability None

[Learn more about base metrics](#)

CVSS:4.0/AV:L/AC:L/AT:N/PR:L/UI:N/VC:L/VI:L/VA:N/SC:N/SI:N/SA:N

**CVE ID**

CVE-2026-34450

**Weaknesses**

- ▶ CWE-276
- ▶ CWE-732

**Credits**



**gn00295120**

Finder